Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 21 (2013) 107 – 113

Procedia Computer Science

The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013)

An Autonomic Agent Trust Model for IoT systems

X. Xu[a,c,*], N. Bessis[b], J. Cao[a]

[a] College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, China
[b] School of Computing and Mathematics, University of Derby, Derby, United Kingdom
[c] State Key Laboratory for Novel Software Technology，Nanjing University, Nanjing, China

Abstract

The IoT systems encounter more serious issues of security, reliability and availability. In this paper, we propose an autonomic agent trust model to decrease security concerns, increase reliability and credibility and ensure information collecting, sharing and processing in dynamic IoT environments. In order to build the credibility protection model for IoT systems, agents and agent platforms have to be built on all nodes. Agent-based node in IoT systems is independent, self-governing software and hardware integrated system. Introducing the agent technology to build systems could manage resources and regulate actions of node in order to maximize the benefit of the whole IoT system. Firstly, we analyze on the credibility of IoT systems and explain why IoT systems are difficult to achieve safe and reliable computing and service quality assurance mechanisms. Secondly, we provide the architecture of trustable agent and agency. After that, we propose a novel architecture named TAEC (Trustworthy Agent Execution Chip), which is to use the high-security, cost-effective software and hardware platform for the safe operation of Agent. The proposed approach is to install TAEC on each sensor node, which provides autonomic trusted hardware execution environment for agents.

Keywords: Autonomic Agent; Trust model; Internet of Things.

1. Introduction

The Internet of Things (IoT) is an emerging paradigm shaping our current understanding about the future of Internet. IoT has been emerged as one of the most important paradigmatic strings of thought

* Corresponding author. Tel.: +86-13813885172; fax: +86-25-85866433.
E-mail address: xuxl@njupt.edu.cn.

doi:10.1016/j.procs.2013.09.016

with regards to the future state of Internet. In a more comprehensive way, IoT transforms real world objects into smart objects and connect them through Internet. In contrast with current Internet, IoT depends on a dynamic architecture where physical objects with embedded sensors will communicate with an e-infrastructure (i.e. a cloud) to send and analyze data using IP [1-3]. While there are several benefits arising from an IoT setting [4], there are also notable challenges such as those related to security, trust and privacy [5].

For example, current research works indicate that Internet of Things (IoT) environments have some unique characteristics [6,7], such as heterogeneity, autonomy, distribution and openness, which may lead to serious security concerns and compromised credibility [8]. For example, malicious subjects could pose serious threats to the normal operations of networks and damage the credibility of networks through fake services, conspiracy, non-cooperation and other malicious behavior [9,10]. As a whole, the construction and operation of IoT systems encounter more serious issues of security, reliability and availability [11].

In order to decrease security concerns, increase reliability and credibility and ensure information collecting, sharing and processing in dynamic IoT environments, we propose an autonomic agent trust model.

According to the definition of FIPA (Foundation for the Intelligent Physical Agent), an agent is a kind of entity with autonomy, activity, mobility, reactivity, sociality, intelligence and other anthropomorphic features [12-15]. Using the agent technology to build the credibility protection model for IoT systems, it means that agents and agent platforms have to be built on all nodes. This means that using a group of decentralized, loosely coupled distributed intelligent agents in IoT environments to achieve the high-efficient intra-or-inter-group collaboration and effective solution to solve a variety of conflicts and contradictions, and thus simulate organizations of human society to solve various problems. However, not all agents have to have all the same components. For instance, agents deployed on cluster servers can have more functions to accomplish more jobs, while agents deployed on sensor nodes can be lighter, with less function and less resource required, which means agent-based IoT systems can achieve a better balance between performance and function.

Agent-based node in IoT systems is independent, self-governing software and hardware integrated system. We suggest introducing the agent technology to build systems with better performance, which could manage resources and regulate actions of node in order to maximize the benefit of the whole IoT system.

Within this context, Section 2 presents an analysis about IoT systems credibility. In Section 3, we will present the architecture of Trustable Agent and Agency. Section 4 presents a novel architecture named TAEC to provide a reliable platform for the safe operation of Agent.

2. Analysis on the credibility of IoT systems

The basic elements of an IoT system are all kinds of nodes, including sensor nodes and cluster server nodes. IoT systems and their nodes have the following features [16-20]:

- Resource redundancy: the number of sensor nodes and server nodes in an IoT system might be really huge, which means failed nodes should not affect the operation and/or the stability of the system as a whole.
- Information duplication: different sensor nodes may collect information about the same object, which means duplicated information must be filtered to define the useful ones.
- Capacity difference: software and hardware resources owned by nodes are very different in quality and quantity.
- Node dynamic and network instability: nodes can join or leave the IoT system dynamically; nodes can also self-decide (autonomously) how and when will provide services, which makes the system very fluid.

- Lack of centralized control node: some IoT systems do not have the centralized control node which can manage the whole system efficiently.

The open integrated IoT systems are difficult to achieve safe and reliable computing and service quality assurance mechanisms due to the following reasons:

(1) Codes and data of tasks transmitting in heterogeneous networks may be attacked or stolen by malicious nodes and/or by malicious execution environments.
(2) Viruses and other malicious codes hidden inside task programs may attack, destroy execution environments or network systems.
(3) Task codes from different users may attack each other and steal information from each other.

In order to protect the transmission of code and data, we can rely on traditional network security technologies, which are mature and effective. For the problem of viruses attacking execution environments and host systems, there is a series of research results and effective methods available, such as the sandbox, digital signature, authentication, authorization and resource allocation, proof code carrying, code inspection and audit [21-24]. However, it is more challenging to protect task codes and data attacked by execution environments and host systems. For example, when a task is transferred and deployed to a destination host to be executed, the initiator of the task would completely loose the control of the task, and each line of the task code must be completely exposed, interpreted and executed in the host system. Task executor can easily isolate, control and attack task codes. For example, a malicious host can extract the private code or data of the task to understand the overall execution logic, spy the workflow and tamper codes and data according to their own will. This especially affects those tasks which have private computing demands.

3. A Case for a Trustable Agent model

Agent runs in the agency, which is the running container of agent, providing the communication service, the registration service, the management capability, the migration function, the persistence service and the security and reliability protection mechanism. With the introduction of the agent, all the sub-tasks can be encapsulated in agents. It is clear that the security basis to achieve the trustworthy virtual private cloud turns to protect the security and reliability on the execution, storage and communication of agent, which means to build the trustable agent and agency, as proposed and shown in Fig. 1.

The proposed Trustable Agent consists of three parts:

- Task entity encapsulating codes and data, including Agent initial program, event handler, and action of implementation.
- Attributes, states and other ancillary modules, including the Agent ID, the attributes (including Agent creator, creation time, etc), the states (recording the current state during the execution of Agent, saving gained knowledge and results, supporting the cross-platform persistent mechanism), ACL (Agent Communication Language), the routing table (the Agent migration path in networks) and the rule strategies.
- Security and reliability protection module, including the encryption and decryption module, the verification code module (to protect the implementation results), the redundancy module, the trustworthiness estimation module, the self-destruction module (responsible for destructing private information of task), the trust certificate (responsible for providing authentication and the note of local resources when enter Agency) and the Trustable Agent interface (to keep illegal access away from outside to Agent).

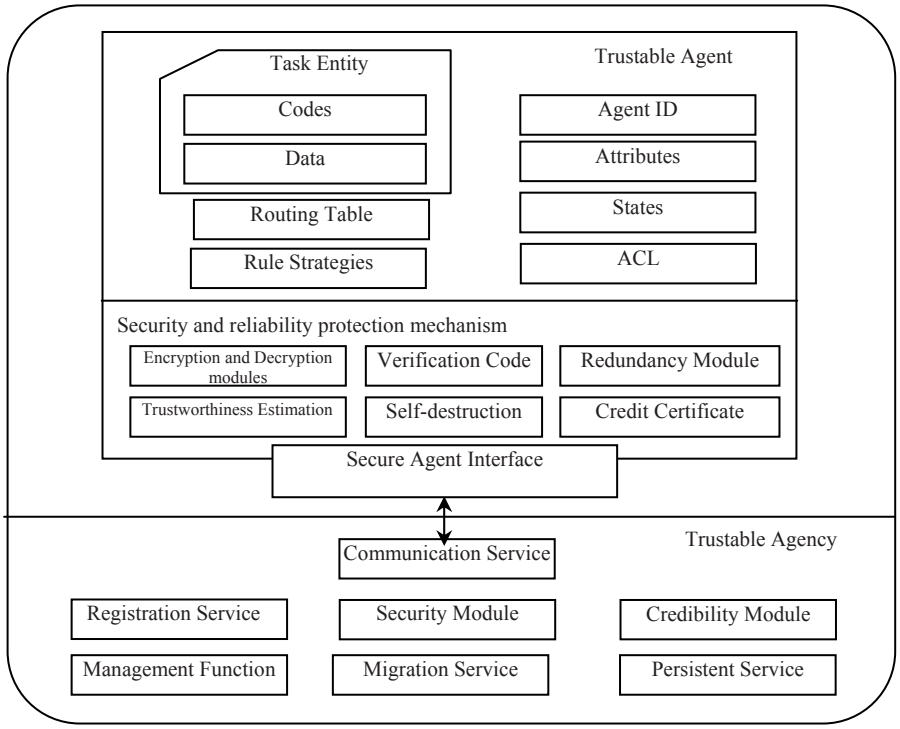

Fig. 1. The Architecture of Trustable Agent and Agency [25]

4. Towards a Trusted Hardware Execution environment for Agent

In the Agent-based IoT system, we have to embed Agents into sensor nodes. Here, we propose a novel architecture named TAEC (Trustworthy Agent Execution Chip). The core idea of TAEC is to use the high-security, cost-effective software and hardware platform for the safe operation of Agent. The proposed approach is to install TAEC on each sensor node, which provides autonomic trusted hardware execution environment for Agent.

Agent can run on the TAEC platform to complete its tasks. The TAEC plays double benefits: protecting nodes and protecting Agents. First of all, the location of an Agent is changed to the secure operating environment of TAEC in the protection of the Agent. Sensor node communicates with TAEC by dedicated or common standardized interfaces and devices, which cannot get programs and data of Agent in TAEC. Then, sensor nodes do not have to provide Agency, while TAEC becomes the only Agent execution environment. Of course, TAEC still needs to send messages to or receive messages from the sensor node.

Fig. 2 shows the architecture of TAEC by illustrating the following five service levels:

(1) The top layer is composed of Agent and Agency. If an Agent migrates to the local node, it will be immediately transferred into TAEC through the standard communication interface. Agent can be protected with encryption, digital signature and other security technologies. One Agency can provide several individual private spaces and encryption, decryption and verification services, ensuring multi-Agent running on the same Agency facilities in their own space independently.

(2) The second layer is the programming function library, which provides required functions to achieve a variety of tasks for Agent-based applications. The library can be added with new functions, modified and upgraded on demand.

(3) The third layer is about embedded operating system running on TAEC hardware platform, which major task is to control the operation and management of the Agent, TAEC system and software and hardware resources.
(4) The bottom layer includes processor, memory, storage device, interface devices, communication module and peripheral circuits to achieve the most basic computing, storage and communication functions.

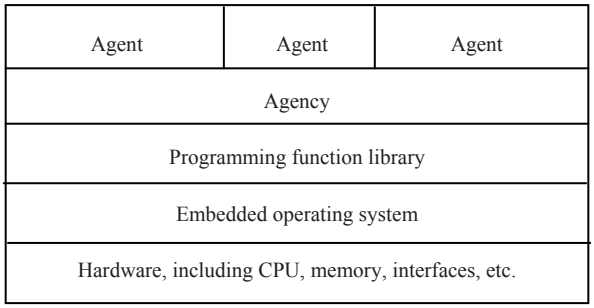

Fig. 2. The architecture of TAEC [26]

5. An Autonomic Agent Trust Model for IoT systems based on TAEC

Fig 3 shows that the proposed model can function either in an IoT centralized-topology or distributed-topology. Each sensor node can register its node name, network address, security requirement, and digital certificate. The latter is issued by the TAEC manufacturer (TAECM).

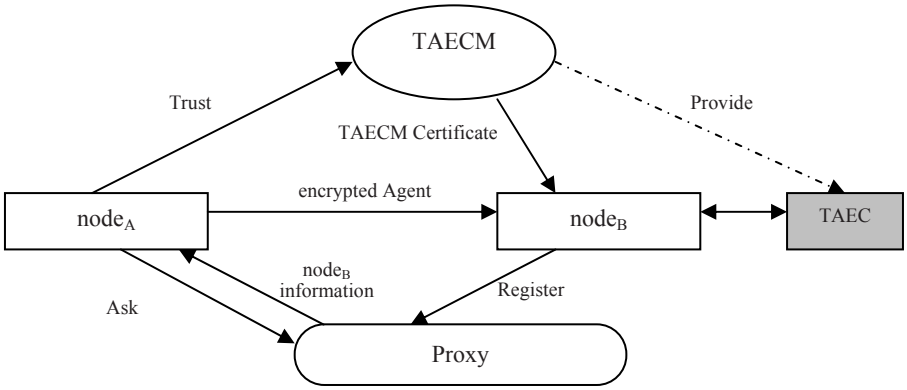

Fig. 3. Agent Protection schematic based on TAEC

The TAECM certificate contains the following information (TAECM, TAEC Type, Security Strategies provided by TAEC, TAEC Public Key).

Sensor node has a copy of TAEC public key to verify the digital certificate issued by the TAECM. TAEC is responsible to utilize the specific encryption co-processor to generate the pair key to ensure that the private key cannot be spied by anyone.

If TAECM has a good reputation, which has already been recognized trustworthy widely, the node owners can trust that TAECM will design and produce such equipment, and will purchase TAEC with

digital certificate. Agent can immigrate and locate at the remote sensor node equipped with TAEC.Based on the trustworthy feature of TAEC manufacturers, nodes with TAEC constitute a safe, credible IoT system. All nodes cooperate with each other based on trustable Agent operation on TAEC, which means that the trust on TAECM replaces the trust relationship among IoT nodes. TAECM can achieve complete security solutions, monitored by the authority, and has independent interest with TAEC buyers.

6. System Construction and Performance Analysis

From what has been discussed above, we can see that the core of the proposed model is TAEC. We chose the silicon chip with complete system architecture and function to be the underlying hardware of TAEC system, which is actually a complete, stand-alone computing and storage platform based on the deep sub-micron silicon semiconductor processing technology. We selected the embedded Linux operating system to be the operating system running on TAEC hardware platform. Both Agent and Agency can be developed with the embedded JAVA technology. Here we specifically chose J2ME (Java 2 Micro Edition) to be the development tool. To ensure Agents not able to interfere with each other, we adopted the sofeware firewall technology to isolate Agents.

The Agent Protection model based on TAEC has the following features:

- Platform independenc. TAEC limits the Agent operating environment inside a chip, which makes the hardware platforms and operating systems of network nodes with TAEC independent of the Agent operating environment. At the same time, TAEC systems developed with the same development standard can run on chips produced by different manufactures, which makes Agent be able to run without restricting the types of underlying silicon.
- Multi-function. Multiple Agents can run in a single TAEC chip. Different Agents can achieve different tasks with different functions.
- Easy to upgrade. TAEC can keep being upgraded with new systems and installed with new applications through the input interface after issued. This feature allows TAEC publishers dynamic to response to the changing customer demands.
- Flexibility. Agent and TAEC system are developed with the embedded object-oriented methods and development tools, which provides the on-chip programming flexibility.
- Compatibility. TAEC is compatible with the international SoC standards as well as industry standards. This compatibility enhances interoperability of Agents and TAECs developed by different manufacturers, making TAEC systems easier to deploy widely in networks.

7. In Conclusion

The architecture and components of the Autonomic Agent Trust Model for IoT systems based on TAEC are proposed in this paper. Our future work involves researching on the proposed model's detailed work procedure and its application demo. We will also plan to design a new dynamic composite credibility evaluation mechanism, including the credit indexes of agent and node computing algorithm and the credibility differentiation strategy. Finally, we will work towards a novel composite collaborative management mechanism based on trusted autonomic agents in order to ensure the efficiency and success rate of the task implementation in IoT environment. Several simulation experiments will be performed to evaluate our proposed model's credibility levels.

Acknowledgements

The subject is sponsored by the National Natural Science Foundation of China (No. 61202004), the China Postdoctoral Science Foundation funded project (Nos.2011M500095 and 2012T50514), the Natural

Science Foundation of Jiangsu Province (No. BK2011754), the Jiangsu Postdoctoral Science Foundation funded project (No. 1102103C) and the Natural Science Fund of Higher Education of Jiangsu Province (No. 12KJB520007).

References

[1] Atzori L, Iera A, Morabito G. The Internet of Things: A survey. *Computer Networks*; 2010, 54(15):2787-2805.
[2] Presser M, Gluhak A. The Internet of Things: Connecting the Real World with the Digital World. *EURESCOM message – The Magazine for Telecom Insiders*; vol. 2, 2009.
[3] Tan L, Wang N. Future Internet: The Internet of Things. *Advanced Computer Theory and Engineering (ICACTE)*, *2010 3rd International Conference* ; p. 376-380, 20-22 Aug. 2010.
[4] Zelenkauskaite A, Bessis N, Sotiriadis S, Asimakopoulou E. Interconnectedness of Complex systems of Internet of Things through Social Network Analysis for Disaster Management. *Proceedings of 4th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS-2012)*; 2012, p. 503-508.
[5] Bassi A, Horn G. Internet of Things in 2020: Roadmap for the Future, EPoSS, Brussels , EU http://www.umic.pt/images/stories/publicacoes2/Internet-of-Things_in_2020_EC-PoSS_Workshop_Report_2008_v3.pdf; 2008.
[6] International Telecommunication Union, Internet Reports 2005: The Internet of things. Geneva: ITU, 2005.
[7] Shen SB, Fan QL, Zong P, et al. Study on the architecture and associated technologies for internet of things . *Journal of Nanjing University of Posts and Telecommunications*; 2009, 29(6): 1-11.
[8] Hu XD. The security of the Internet of Things. Beijing: Science Press; 2012.
[9] Weber RH, Internet of Things New security and privacy challenges. *Computer Law & Security Review*; 2010, 26: 23-30.
[10] Medaglia CM, Serbanati A. An overview of privacy and security issues in the Internet of Things. *Proceedings of the 20th Tyrrhenian Workshop on Digital Communications,* Sardinia, Italy; 2010, p. 389-394.
[11] Wu ZQ, Zhou YW, Ma JF. A Security Transmission Model for Internet of Things. *Chinese Journal of Computers*; 2011, 34(8): 1351-1364.
[12] FIPA. FIPA abstract architecture specification. Available from: http://www. fipa.org/ specs/fipa00001/SC00001L.html; 2002.
[13] Telecom Italia SpA. Jade-Java Agent Development Framework. http://jade.tilab.com/;2009.
[14] Shi ZZ. Intelligent Agent and Its Applications. Beijing: Science publishing company; 2000.
[15] Wooldridge M. An Introduction to Multi-Agent Systems. Chichester, England: John Wiley & Sons; 2002.
[16] Commission of the European communities, COM (2009)278 final. Internet of things-an action plan for Europe, Brussels; 2009. http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf.
[17] Liu YH. From pervasive computing, CPS to the Internet of things: next generation Internet vision .*Communications of the CCF*; 2009, 5(12): 66-69.
[18] Leusse P, Periorellis P, Dimitrakos T, et al. Self Managed Security Cell, a security model for the Internet of Things and Services. *Proceedings of the 2009 First International Conference on Advances in Future Internet*, Piscataway; 2009, p. 47- 52.
[19] European Research Projects on the Internet of Things(CERP-IoT) Strategic Research Agenda (SRA). Internet of things strategic research roadmap;2009. http://ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf.
[20] Cristeal V, Dobre C, Pop F. Context-Aware Environments for the Internet of Things. In: Bessis N, et al. ed.. *Internet of Things & Inter-cooperative Computing Technology*, Berlin Heidelberg: Springer-Verlag; 2013.
[21] Fritz H. Time limited blackbox security: Protecting mobile agents from malicious hosts. In: Vigna, Giovanni ed.. *Mobile Agents and Security*, LNCS 1419, Springer-Verlag;1998.
[22] Sander T, Tschudin CF. Protecting Mobile Agents Against Malicious Hosts, Mobile agents and security. *Lecture Notes in Computer Science*. New York: Springer-Verlag; 1998, 14(19):44--60.
[23] Zhao L, Wang FX, Liu ZP, Chang Z. Construction of sand box in computer immune system . *Journal of Dalian University of Technology*; 2003,43 (s1):9-11.
[24] Wang RC, Zhao XN, Wang SD, Sun ZX. Analysis and research of Mobile Agent system security framework based network. *Journal of Computer*; 2003,26 (4):478-483
[25] Xu XL, Cheng CL, Xiong JY, Wang RC. Mobile agent-based secure task partitioning and allocation algorithm for cloud & client computing. *Transaction of Beijing Institute of Technology*; 2011,31(8): 922~926.
[26] Xu XL, Cheng CL, Chen DW, Xiong JY. Research on model of trusted agent-on-chip for P2P networks. *Computer Technology and Development*; 2010, 20(9):140-144.